PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161165
(43)Date of publication of application : 18.06.1999

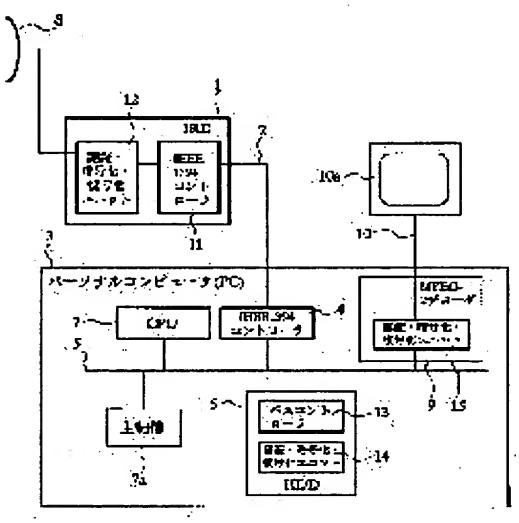
(51)Int.Cl. G09C 1/00
G06F 13/00
H04L 9/32

(21)Application number : 09-325768
(22)Date of filing : 27.11.1997

(71)Applicant : HITACHI LTD
(72)Inventor : FURUKAWA ISAO

(54) INFORMATION PROCESSING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an unauthorized access to the data which are handled by the information processing device.
SOLUTION: The device composed of a PC3 and an antenna 8 which receives pay satellite broadcasting signals, etc., and an IRD (a digital satellite broadcasting tuner) 1, both of which are connected to the PC3 through an IEEE 1394 bus 2. IN the PC3, an IEEE 1394 controller 4 which conducts an I/F control of the IEEE 1394 bus 2, a storage device (HDD) 6 which stores the data, etc., received by the IRD 1, a CPU 7 which controls the entire system, a main storage 7a and a MPEG-2 decoder 9 for contents reproducing, etc., are connected through a PCI bus 5. In such a constitution, each of the HDD6, the IRD1 and the decoder 9 is provided with a certifying.ciphering.deciphering unit 14, that certifies the party to which data are transmitted, and certifying.ciphering.deciphering units 12 and 15. Then, certifying of each among the units 12, 14 and 15 and data ciphering/deciphering of the data, which are flowing in the data transfer paths including the buses 2 and 5, are conducted.



LEGAL STATUS

[Date of request for examination] 31.08.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－161165

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ
Ｇ０６Ｆ　13/00	３５７	Ｇ０６Ｆ　13/00	３５７Ａ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ

審査請求　未請求　請求項の数１　ＯＬ　（全８頁）

(21)出願番号　特願平9－325768

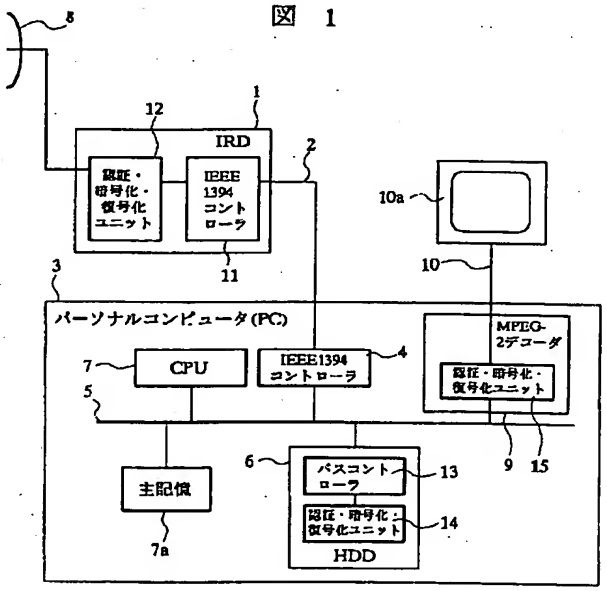
(22)出願日　平成９年(1997)11月27日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　古川　勲
神奈川県海老名市下今泉810番地　株式会社日立製作所オフィスシステム事業部内
(74)代理人　弁理士　筒井　大和

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】　情報処理機器にて取り扱われるデータの不正使用を防止する。
【解決手段】　ＰＣＩバス５を介して、ＩＥＥＥ１３９４バス２とのＩ／Ｆ制御等を行うＩＥＥＥ１３９４コントローラ４、ＩＲＤ１にて受信されたデータ等の格納を行う記憶装置（ＨＤＤ）６、全体の制御を行うＣＰＵ７、主記憶７ａ、コンテンツ再生用のＭＰＥＧ－２デコーダ９等を接続した構成のＰＣ３に、有料衛星放送等の受信を行うアンテナ８、ＩＲＤ１をＩＥＥＥ１３９４バス２を介して接続した構成において、ＨＤＤ６、ＩＲＤ１、ＭＰＥＧ－２デコーダ９の各々には、データの送信相手の認証等の動作を行う認証・暗号化・復号化ユニット１４、認証・暗号化・復号化ユニット１２、認証・暗号化・復号化ユニット１５を設け、これら３者間における互いに他の認証、ＩＥＥＥ１３９４バス２やＰＣＩバス５等のデータ転送路を流れるデータの暗号化／復号化を行うようにした。

図　1



2：IEEE1394バス　10：アナログTV出力
5：PCIバス　10a：ディスプレイ
8：アンテナ

【特許請求の範囲】
【請求項１】　所望の情報伝送路を介して記憶装置と周辺機器とが接続された構成の情報処理装置であって、
前記記憶装置および前記周辺機器の各々には、前記情報伝送路を経由して情報の授受を行う相手側を認証する第１の機能、および前記情報伝送路を経由して授受される前記情報の暗号化および復号化を行う第２の機能の少なくとも一方を備えたことを特徴とする情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理技術に関し、特に、たとえばパーソナルコンピュータ等の情報処理機器にて取り扱われるディジタルコンテンツ等のデータの保護に適用して有効な技術に関する。
【０００２】
【従来の技術】映画や音楽などの多量のデータを不正コピーから守る技術として、コピープロテクトのための技術が多数開発されている。代表的なものはビデオテープにおけるアナログコピープロテクトで、ＮＴＳＣ規格の映像信号に規格外の信号を与え、ビデオの誤動作を引き起こすものである。代表的なものとしてＭａｃｒｏＶｉｓｉｏｎ社のプロテクトがある。また、ＤＡＴ（Ｄｉｇｉｔａｌ　ＡｕｄｉｏＴａｐｅ）の場合は、世代管理のための記憶領域が設けられており、コピー不能、１回のみコピー可能、何回でもコピー可能といったようにコピー世代を指定できる。これは、データ自体への暗号化は為されておらず、ＤＡＴの機械には必ずコピー管理機構を設けることを義務づけること、および媒体であるテープへ一定の課金をするという手法をとっている。また、デジタル衛星放送の一つであるＰｅｒｆｅｃＴＶ！においては、ＰｅｒｆｅｃＣａｒｄと呼ばれるＩＣカードをＩＲＤ（デジタル衛星放送チューナ）に差し込まないと有料放送が見れない、というガードがある。ＩＣカードには固有のＩＤがあり、特定のチャネルには特定のＰｅｒｆｅｃＣａｒｄのＩＤしか見れないように放送局側で規制している。ＩＲＤはＰｅｒｆｅｃＣａｒｄのＩＤと番組情報から、これをデコードして良いか判断するものである。
【０００３】一方、コンピュータの世界では、また別のコピープロテクト技術がある。代表的なものとしては、以下のようなものがある。
【０００４】ＣＤ－ＲＯＭやＦＤの分野では、物理フォーマットの特性を利用したプロテクトが行われている。これは、規格外のＦＤやＣＤ－ＲＯＭを作り、コントローラ等のハードウェアをプログラム自らが制御して、本来読めないはずの規格外のエリアにあるデータがあるかどうかで正規のメディアかどうかを確認するものである。
【０００５】また、比較的高価なＣＡＤソフトの一部では、ＰＣ（パーソナルコンピュータ）のパラレルポートに接続する専用キーデバイスによるプロテクトがある。これは、ＣＡＤソフトの販売元から正規のユーザに配付され、パラレルポートに接続するコネクタの形状を呈する認証装置であり、やはり固有のＩＤを持っている。ＣＡＤソフトはパラレルポートに装着されたこの認証装置のＩＤを読み取り、正規のＩＤ（ユーザ）であるかどうかを判断して動作するかどうかを決めるというものである。
【０００６】ソフトのインストールや起動の際にパスワードを入力するという手法も広く行われている。
【０００７】ＤＶＤやデジタル衛星放送の出現により、映像や音声、データなどのコンテンツがデジタルで配信される機会が急速に広まっている。次世代ＩＲＤでは、このためのＩＲＤからのデジタルデータの出力の規格としてＩＥＥＥ１３９４を使用することがほぼ確定している。ＩＥＥＥ１３９４は次世代の高速シリアルバスの一つであり、４００Ｍｂｐｓ以上の伝送速度とＰｌｕｇ　＆　Ｐｌａｙ、ＨｏｔＰｌｕｇの機能を実現したバスである。また、放送の種類として、従来の音声、映像のみではなく、ＰＣ（パーソナルコンピュータ）等の個人用の情報処理機器での使用を前提としたデータ放送の予定もある。また、デジタルＶＴＲ、デジタルオーディオアンプ、等のＡＶ機器にもＩＥＥＥ１３９４が搭載される見込みである。
【０００８】デジタルでのコピーは、いくらコピーしてもデータの劣化がないため、最初にコピーを許してしまうと後は高品質のデータのコピーし放題になるという重大な問題がある。よって、従来以上にコピープロテクトには気を使わなければならなくなる。従来の技術では、ＩＲＤからのデータ放送は、コピープロテクトという観点ではさまざまな問題を抱えている。以下にその内容を示す。
【０００９】
【発明が解決しようとする課題】ユーザが暗証番号を入れる方法では暗証番号を一緒にコピーされたりアタックされる可能性がある。これは、ユーザが入れられる暗証番号の桁数は一般的に短いことに起因するものである。また、パラレルポートに接続する、あるいはＰｅｒｆｅｃＣａｒｄのような特殊なハードウェアを使う場合では、そのハードウェアが繋がっている閉じたシステムでしか使用できないし、次々と新しいデータが降り注いでくる放送に対応するハードウェアを作り続けるのは事実上不可能である。これらは、特にＰＣでの使用を前提とした場合、致命的な欠点となる。
【００１０】ＩＲＤの場合、ＩＥＥＥ１３９４によるデータ伝送が前提となるため、ＦＤやＣＤ－ＲＯＭで使われていたような物理フォーマットの規格外の使い方や、ＭａｃｒｏＶｉｓｉｏｎにあるような映像信号の規格外の信号を使うような、媒体や通信路の物理特性を利用したプロテクトは利用できない。

【００１１】ＩＥＥＥ１３９４は、そのプロトコルの性質上、１対１通信であっても、全てのノードにそのデータが見えてしまう。よって、プロトコルアナライザなどによるデータの横取りが可能である。また、ＩＥＥＥ１３９４はスターおよびツリー構造の接続が可能であり、またＰｌｕｇ　＆　Ｐｌａｙ、Ｈｏｔ　Ｐｌｕｇ機能を有しているので、ＰＣをその通信網に後から接続することは簡単に出来てしまう。つまり、ＩＲＤなどのＡＶ機器のデジタル出力は、ＰＣがＩＥＥＥ１３９４接続のどこかに接続することで見れてしまう。

【００１２】この問題に対する対策として、ＩＥＥＥ１３９４におけるコピープロテクト技術は進展中である。ＩＥＥＥ１３９４に接続されたどのデバイス同士でも、他の接続したデバイスによる盗み見に対し安全なデータの授受が出来る。これは現在規格策定中であり、どの程度の暗号化が為されるかは未定になっている。ただし、何れにしても、このコピープロテクトは伝送路の暗号化に限定されている。従って、装置の内部ではこれは解読され、平文として装置内部を流れたり蓄積される。完成民生機器の場合はＤＡＴ等の例に見られるようにある程度メーカで対応できるが、ＰＣ用のデータ放送も考えられており、またＰＣでのＡＶコンテンツ再生も可能であることから、ＰＣ接続は考慮する必要がある。ＰＣ接続においては、以下のような問題が生じる。

【００１３】ＰＣはハードウェア、ソフトウェアの交換、増設がユーザレベルで可能なため、ＤＡＴのようなコピープロテクトでは、暗号化されていないデータがＰＣ内部を流れる際、そのデータを横取りして世代管理領域を書き換えるなどの不正が非常に簡単に行える。また、暗号化をしても、これを解読するためのプログラムは開発可能であるため、安易な暗号化は危険である。特に暗号キーのやり取りをする際にキーを盗み見されると、いくら暗号化しても意味が無い。従来のＰＣの場合、どのようなアルゴリズムを駆使してやり取りをしても、その暗号キーは少なくともメモリ上のどこかに存在し、ないしはＰＣの内部バスであるＰＣＩバスなどを必ず通ることになるので、これを盗み見される可能性は否定できない。

【００１４】即ち、コンテンツがＰＣに取り込まれた際、メモリ、ＰＣＩバス、ハードディスク、ＤＶＤ－ＲＡＭなどの何れかには必ず平文（暗号化されていない）データが存在し、また暗号化されていない鍵が存在する。このデータを別の媒体にコピーすることはプログラム的には極めて簡単で、更にこのプログラムをネットワーク上で配布したりウィルスに仕立てるなどして広めることも簡単に可能である。よって、データをＰＣで取り込むというだけで、不正コピーの可能性が従来に比べて飛躍的に高くなることになる。

【００１５】また、デジタル衛星放送のコンテンツをＰＣで使用する際には、はじめからＰＣでの使用が前提となるが、将来ＩＥＥＥ１３９４が高度な暗号化をして通信路での安全性を確保しても、ＰＣ内部での使用においてＰＣＩバスの部分に解読後のデータが流れることになるので、ウィルスなどの悪意のあるプログラムから守ることが出来ない。

【００１６】これに対して、ＤＶＤ－ＲＯＭが使用している手法は、比較的安全であるとされる。ＤＶＤドライブと、データを出力するＭＰＥＧ－２デコーダボードの間はＰＣＩバスおよびＩＤＥバスが介在するが、この間の通信は「認証」と呼ばれるプロセスを経た後、この認証によって作成した暗号キーを使って暗号化した上で送信する。

【００１７】認証は、暗号化技術の手法としては一般的なものである。これは、認証をする各々が、盗み見される可能性のある通信路のみを使って通信し、お互いが信頼できる相手であることを確認するための手法である。最も簡単なものとしては、公開暗号鍵の手法を用いるものがある。これは、自分の秘密鍵で自分が発生させた乱数を暗号化して相手に送り、相手側にこれを解読させて相手側に相手側の秘密鍵で暗号化して自分に送らせ、これを解読して最初の乱数と一致するかどうかを見る、というものである。ＤＶＤの場合ではもう少し複雑で、認証をしようとする二者が公平な第三者である認証機関より秘密鍵と公開鍵の提供を受け、認証作業において、これが第三者から提供されたものであることを確認するためのアルゴリズムが加わる。これらのアルゴリズムの特徴は、通信路を盗み見してもそのデータは暗号化されており、しかもそれを解くための鍵はソフトウェア的に解析できないところに置かれる（通常はＲＯＭに焼かれる）ため、ハードウェアを分解するなどしない限り解読困難である。こうして認証を行った後、その認証情報を元にしてお互いが暗号鍵を内部で生成し、実際のデータはこの暗号鍵を使って暗号化した上でやり取りする。このため、実際のデータを暗号化する暗号鍵は通信路に現れないため、第三者による鍵の入手は不可能になる。

【００１８】従来例として最も本発明に近い上記のＤＶＤ－ＲＯＭにおける手法では、通常のコマンドでは見ることが出来ないメディア固有のＩＤ領域、コンテンツ毎の暗号キー領域が設定されており、メディアをどのドライブに入れてもこの情報を単独で読み出すことは出来ない、という特性を利用している。これにより、認証のための情報や暗号キーはドライブによりコントロールされる。しかし、放送や通信を前提とした場合は、認証や暗号化・復号化に必要な情報は全て放送や通信で送る必要がある。このため、ＤＶＤ－ＲＯＭにおける「通常のコマンドでは見ることが出来ない」という条件が崩れ、通信路をスヌープすることにより暗号キーを盗まれる可能性が飛躍的に高まるため、使用することが出来ない。

【００１９】また、もし安全にデータを蓄積できた場合でも、それを活用する段階で同じようにデータがメモリ

にロードされると同様の問題が生じてしまう。ロードの段階でＰＣＩバスおよびメモリに平文データが現れてしまうため、これを盗まれる可能性が生じる。

【００２０】以上のように、ＩＲＤからＰＣ等の情報処理機器へデータ伝送をする場合、従来の技術ではコピープロテクト技術は不十分である。

【００２１】本発明の目的は、パーソナルコンピュータ等の情報処理機器にて取り扱われるコンテンツデータやプログラム等の不正使用を防止することが可能な情報処理技術を提供することにある。

【００２２】本発明の他の目的は、不正使用を懸念することなく、パーソナルコンピュータ等の情報処理機器を用いたコンテンツデータやプログラム等の処理システムの構築を実現することが可能な情報処理技術を提供することにある。

【００２３】

【課題を解決するための手段】本発明では、所望の情報伝送路を介して記憶装置と任意の周辺機器の間、および周辺機器間にて情報の授受を行うように構成された情報処理装置において、記憶装置および周辺機器の各々には、情報伝送路を経由して情報の授受を行う相手側を認証する第１の機能、および情報伝送路を経由して授受される情報の暗号化および復号化を行う第２の機能の少なくとも一方を備えた構成とする。

【００２４】より具体的には、一例として、ＰＣにてＩＲＤ等を備えた有料衛星放送の受信システムを構築する場合、ＰＣ内部にあるＨＤＤを、認証と暗号化の機能を搭載したインテリジェントタイプとする。ＩＲＤ側にも認証機能を持たせ、ＨＤＤへは暗号化して送信する。ＨＤＤからコンテンツ等のデータを、プログラムやＭＰＥＧ－２デコーダなどの外部に出す際は、その相手との認証を行い、暗号化してデータを渡す。データを渡された相手は、コピーからの防衛を行いつつデータを処理する。これにより、バス等のデータ転送経路を通るデータを全て暗号化し、かつ暗号鍵そのものも暗号化してやり取り出来るため、安全なデータ伝送が出来る。

【００２５】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【００２６】（実施の形態１）図１は、本発明の一実施の形態である情報処理装置の構成の一例を示す概念図である。本実施の形態では、一例として、パーソナルコンピュータ等の情報処理装置を用いて、たとえば有料衛星放送の受信システムを構成する場合を例に採って説明する。

【００２７】有料衛星放送等の受信を行うアンテナ８は有料衛星放送のセキュリティ管理等を行うＩＲＤ１に接続されており、さらにＩＲＤ１はＩＥＥＥ１３９４バス２を通してパーソナルコンピュータ（ＰＣ）３に接続している。

【００２８】ＰＣ３の内部では、一例として、ＰＣＩバス５を介して、ＩＥＥＥ１３９４バス２とのＩ／Ｆ制御等を行うＩＥＥＥ１３９４コントローラ４、ＩＲＤ１にて受信されたデータ等の格納を行う記憶装置（ＨＤＤ）６、全体の制御を行うＣＰＵ７、ＣＰＵ７を制御するプログラムやデータ等が格納される主記憶７ａ等を接続した構成となっている。

【００２９】本実施の形態の場合、ＩＲＤ１は内部にＩＥＥＥ１３９４バス２とのＩ／Ｆ制御等を行うＩＥＥＥ１３９４コントローラ１１と、ＩＥＥＥ１３９４バス２に送出されるデータの暗号化や、データの送信相手の認証等の動作を行う認証・暗号化・復号化ユニット１２を有している。

【００３０】一方、ＨＤＤ６の内部には、ＰＣＩバス５との間のＩ／Ｆ制御を行うバスコントローラ１３と、このバスコントローラ１３を介して外部との間で授受されるデータの暗号化／復号化、さらにはデータ授受の相手の認証等の動作を行う認証・暗号化・復号化ユニット１４を備えている。

【００３１】また、ＰＣ３において、ＰＣＩバス５には、ＭＰＥＧ－２デコーダ９が接続され、このＭＰＥＧ－２デコーダ９は、ＰＣＩバス５を経由して授受されるデータの暗号化／復号化、相手側の認証等の動作を行う認証・暗号化・復号化ユニット１５、が設けられ、復号されたデータは、アナログＴＶ出力１０を経由してディスプレイ１０ａに出力される構成となっている。

【００３２】ＨＤＤ６内部の認証・暗号化・復号化ユニット１４は、ＩＲＤ１内部の認証・暗号化・復号化ユニット１２との間で、ＩＥＥＥ１３９４コントローラ１１、ＩＥＥＥ１３９４バス２、ＩＥＥＥ１３９４コントローラ４、ＰＣＩバス５を通じた情報の授受により認証を行い、これによって得たキーで暗号化した上で受信したコンテンツ等のデータをＨＤＤ６に送る。この際、ＩＥＥＥ１３９４バス２、ＰＣＩバス５を経由するのでここでデータを盗み見することは可能であるが、認証を経て暗号化されているので解読できない。

【００３３】本実施の形態の場合、ＩＥＥＥ１３９４規格にのみ頼る暗号化との違いは、ＰＣ３の内部においても暗号化が保たれていることである。ＩＥＥＥ１３９４規格の場合は、ＩＥＥＥ１３９４コントローラ１１とＩＥＥＥ１３９４コントローラ４との間の途中の通信経路のみ暗号化され、ＰＣ３内部のＰＣＩバス５では平文でデータが流れる。即ち、ＰＣＩバス５のスヌープでデータを盗み見ることが出来る。これに対し、本実施の形態では、ＩＲＤ１からＨＤＤ６に送出されるデータは、ＩＲＤ１の側の認証・暗号化・復号化ユニット１２に暗号化された後に送出されるため、ＨＤＤ６の内部に入るまで暗号化されたままなので、ＰＣＩバス５においてもデータを盗み見ることが出来ない。尚、認証の詳細については実施の形態３で説明する。

【００３４】認証を経ない一般的な暗号化では、解読キーが暗号化されないまま信頼できないＰＣＩバス５やＩＥＥＥ１３９４バス２を通ることになるので、解読キーを得た第三者がデータをコピーすることが可能になってしまうが、本実施の形態においてはこれらの信頼できないバスを経由しても解読キーは暗号化して送信されるため、第三者は解読キーを入手することが出来ない。このため第三者がデータを解読するにはキーアタックを行うしかないが、解読キーの長さは幾らでも長く出来るため、危険度に応じてキーを長くすれば安全である。ここで、一般的にはキーの解読はキーの長さに応じて指数関数的に難しくなることが知られていることを指摘しておく。

【００３５】ＨＤＤ６に貯えられたデータは、ＨＤＤ６内部の認証・暗号化・復号化ユニット１４を通じてしかやり取りすることが出来ない。したがって、ユーザは、例え自分のコンピュータといえども、ＨＤＤ６の許可無しにデータを見ることは出来ない点に本実施の形態の大きな特徴がある。

【００３６】（実施の形態２）同じく図１で、ＰＣ３のＨＤＤ６へ蓄積したデータが映像データであった場合のデータ出力処理の一例を説明する。

【００３７】ＨＤＤ６に蓄積されたデータはＰＣＩバス５を通じてＭＰＥＧ－２デコーダ９に送られ、アナログＴＶ出力１０を経由してディスプレイ１０ａに出力される。ＨＤＤ６とＭＰＥＧ－２デコーダ９の間のデータやり取りには、ＨＤＤ６側の認証・暗号化・復号化ユニット１４とＭＰＥＧ－２デコーダ９側の認証・暗号化・復号化ユニット１５との間での認証が必要であり、データは暗号化される。この際、ＰＣＩバス５を経由するが、暗号化されているのでデータは利用できない。また、認証されているので間違った相手にデータを送ることはない。

【００３８】ＨＤＤ６からデータを取り出すにはＨＤＤ６との認証に成功する必要があり、そのためには認証機関より与えられた公開暗号鍵が必要である。即ち、公開暗号鍵をコントロールすることにより、データを使ってよいデバイスが制限される。実際には、公開暗号鍵はＭＰＥＧ－２デコーダ９が持っているが、ＭＰＥＧ－２デコーダ９を製造するメーカが認証機関から鍵を契約により取得する。取得のためには、解読後のデータをボード内部でのみ使うようにハードウェア的な制限を加えるなど、認証機関が与える一定の条件をクリアしなければならないようにする。これにより、コンテンツメーカは、ＰＣ３に送ったデータの使われ方、コピーに関するコントロールを実現できる。

【００３９】これは、ＰＣ３におけるＤＶＤ－Ｖｉｄｅｏの再生の一般的構成と極めて似ているが、データの保存元であるＨＤＤ６は書き換え可能であり、更に記憶媒体が着脱不可能である点が大きく異なる。書き換え可能である点に関しては、ＨＤＤ６が貯えるデータはどこからかコピーしてきたものであるため、少なくともそのデータは純粋に論理的なデータである。つまり、ＣＤ－ＲＯＭやＦＤＤにおける物理的なコピープロテクトは原理的に不可能であり、ＤＶＤ－ＲＯＭにおけるディスクＩＤのような特定のデバイス固有の仕掛けも同様に不可能である。また、記憶媒体が着脱不可能である点に関しては、着脱可能な媒体の場合、媒体のどこに暗号鍵を置いても、外して別の装置に掛けることでその暗号鍵が読めてしまうのに対し、媒体が着脱不可能なのであくまでもＨＤＤ６内部の認証を通してしか情報を入手することが出来ず、暗号鍵は安全である。

【００４０】ＭＰＥＧ－２映像に限らず、データを扱う機器一般にこれは適用できる。例えば相手がＡＣ－３デコーダアンプである場合など、音声データであった場合、認証を経ていないアンプでは再生できない。また、相手がディスプレイであった場合、表示は出来てもアナログ出力が出ないようにする、アナログコピーガードを掛ける、等のコントロールをディスプレイ側ですることが出来るし、認証を得ていないディスプレイでは再生できない。

【００４１】また、複数のＨＤＤの間でコピーをする場合、認証機能の無いＨＤＤにコピーすることは出来ないようにするか、暗号化されたままコピーされるように設定できる。後者では、この復号キーは認証機能のあるＨＤＤのみが所有しているため、最終的にデータを使用するところ、実施の形態２ではＭＰＥＧ－２デコーダ９においてデータを解読することが出来ず、結果としてコンテンツメーカはコピーコントロールが出来たことになる。

【００４２】以上のように、最終的にユーザがデータを使うためのハードウェアを認証機関が指定すること、即ち認証鍵を配布するかしないかをコントロールすることにより、データをユーザが使うための条件をコントロールすることが出来る。

【００４３】（実施の形態３）図２は、本発明の情報処理装置にて使用される認証アルゴリズムの一例を示すフローチャートである。

【００４４】認証は、実施の形態１においてはＩＲＤ１とＨＤＤ６との間で、実施の形態２においてはＨＤＤ６とＭＰＥＧ－２デコーダ９との間で行われる。

【００４５】これは、原則的には一般的に行われている認証のアルゴリズムと同一のものを使える。図２では、最も簡単な例を示している。ＩＲＤ１とＨＤＤ６が認証を行う例を示す。

【００４６】ＩＲＤ１側には秘密鍵Ｋｐｒ（ＩＲＤ）および公開鍵Ｋｐｕ（ＩＲＤ）、ＨＤＤ６側には秘密鍵Ｋｐｒ（ＨＤＤ）および公開鍵Ｋｐｕ（ＨＤＤ）を持つ。また、双方が共通の暗号化アルゴリズムＣ（Ｋｅｙ，Ｄｅｓｔ）および復号化アルゴリズムＣ’（Ｋｅｙ，Ｄｅ

ｓｔ）を持つ。ここでＫｃｙは暗号化鍵、Ｄｅｓｔはターゲットデータである（ステップＳ１）。

【００４７】アルゴリズムＣと公開鍵Ｋｐｕ、秘密鍵Ｋｐｒの間には、以下のような関係がある。即ち、アルゴリズムＣで秘密鍵Ｋｐｒをキーとして暗号化したデータＣ（Ｋｐｒ，Ｄｅｓｔ）に対して公開鍵Ｋｐｕを用いて復号化した結果であるＣ’（ｋｐｕ，Ｃ（Ｋｐｒ，Ｄｅｓｔ））は一致する。またこの逆に、アルゴリズムＣで公開鍵Ｋｐｕをキーとして暗号化したデータＣ（Ｋｐｕ，Ｄｅｓｔ）に対して秘密鍵Ｋｐｒをキーとして復号化した結果であるＣ’（Ｋｐｒ，Ｃ（Ｋｐｕ，Ｄｅｓｔ））は一致する。即ち、秘密鍵で暗号化したデータは公開鍵で解け、公開鍵で暗号化したデータは秘密鍵で解ける。また、アルゴリズム、公開鍵、暗号化されたデータの三つを第三者に知られても、これから平文データないしは暗号鍵を求めることは、数学的に極めて困難である。

【００４８】ＨＤＤ６がＩＲＤ１にデータの転送要求を出す時、ＨＤＤ６はＩＲＤ１に対し、自分の公開鍵Ｋｐｕ（ＨＤＤ）を送信する（ステップＳ２）。

【００４９】ＩＲＤ１はこれを受け取ると、自身で乱数Ｒ（ＩＲＤ）を発生させ、これを種としてＫｐｕ（ＨＤＤ）を暗号化する。これをＣ１＝Ｃ（Ｋｐｕ（ＨＤＤ），Ｒ（ＩＲＤ））と表す（ステップＳ３）。ＩＲＤ１はこの結果を、自分の公開鍵であるＫｐｕ（ＩＲＤ）と共に送信する（ステップＳ４）。

【００５０】ＨＤＤ６は受け取った暗号であるＣ１を自分の暗号鍵で復号化する。これをＲ’（ＩＲＤ）＝Ｃ’（Ｋｐｒ（ＨＤＤ），Ｃ１）で表す。これは、元のＲ（ＩＲＤ）に一致するはずである。ＨＤＤ６はこれを相手の公開鍵Ｋｐｕ（（ＩＲＤ）で暗号化した結果であるＣ２＝Ｃ（Ｋｐｕ）ＩＲＤ），Ｒ（ＩＲＤ））をＩＲＤ１に送信する。同時に、自身で乱数Ｒ（ＨＤＤ）を発生させ、これを相手の公開鍵で暗号化した結果であるＣ３＝Ｃ（Ｋｐｕ（ＩＲＤ），Ｒ（ＨＤＤ））を送信する（ステップＳ５、ステップＳ６）。

【００５１】ＩＲＤ１はＣ２を復号化した結果であるＲ”（ＩＲＤ）＝Ｃ’（Ｋｐｒ（ＩＲＤ），Ｃ２）と最初に自身が発生させた乱数であるＲ（ＩＲＤ）が一致するかどうかを調べる。一致すれば、ＩＲＤ１にとってＨＤＤ６は認証されたことになる。これが成功すると、ＩＲＤ１はＣ３を復号化する。これをＲ’（ＨＤＤ）＝Ｃ’（Ｋｐｒ（ＩＲＤ），Ｃ３）で表す。Ｒ’（ＨＤＤ）はＲ（ＨＤＤ）に一致するはずである。ＩＲＤ１はこれを暗号化してＨＤＤ６に送信する。これをＣ４＝Ｃ（Ｋｐｕ（ＨＤＤ），Ｒ’（ＨＤＤ））で表す。同時に、ＩＲＤ１はデータ送信用のキーであるＫを生成し、Ｃ５＝Ｃ（Ｋｐｕ（ＨＤＤ），Ｋ）として送信する（ステップＳ７、ステップＳ８）。

【００５２】ＨＤＤ６はＣ４を解読し、Ｒ”（ＨＤＤ）＝Ｃ’（Ｋｐｒ（ＨＤＤ），Ｃ４）を生成する。これがＲ（ＨＤＤ）と一致すれば、ＨＤＤ６にとってＩＲＤ１は認証されたことになる。これを受けて、ＨＤＤ６はＫ＝Ｃ’（Ｋｐｒ（ＨＤＤ），Ｃ５）を生成する。

【００５３】以上の操作により、お互いはお互いを認証し、実際のデータ暗号化のための共通キーＫを共有することが出来たことになる。以後のデータ送信は共通鍵暗号アルゴリズムと共通キーＫを使ってやりとりする。

【００５４】たとえば、ＩＲＤ１にて受信した有料衛星放送のコンテンツデータ（Ｄａｔａ）をＩＲＤ１からＨＤＤ６へ送出する場合には、たとえば、図３に例示されるように、データストリームを、たとえば所定のビット長毎に共通キーＫを用いて、認証・暗号化・復号化ユニット１２にて、Ｃ６＝Ｃ（Ｄａｔａ，Ｋ）として暗号化されたデータストリームを生成した後、このＣ６をＨＤＤ６へと送り出す（ステップＳ１０，ステップＳ１１）。

【００５５】このＣ６を受信したＨＤＤ６側では、Ｃ’（Ｃ６，Ｋ）にて、Ｃ６を復号化して元のコンテンツデータ（Ｄａｔａ）を得て記憶媒体に格納する（Ｓ１２）。

【００５６】また、ＨＤＤ６に格納されたコンテンツデータを、ＭＰＥＧ－２デコーダ９に送信する場合には、送信側のＨＤＤ６は、図２におけるＩＲＤ１と等価な動作を行い、受信側のＭＰＥＧ－２デコーダ９は、図２におけるＨＤＤ６と等価な動作を行うことで、ＨＤＤ６とＭＰＥＧ－２デコーダ９は互いに他を認証できるとともに、ＰＣＩバス５を流れるコンテンツデータは両者の固有の共通キーＫにて暗号化された状態となるため、ＰＣＩバス５を流れるコンテンツデータの不正使用を確実に防止できる。

【００５７】同様に、ＩＲＤ１から、ＰＣＩバス５を経由して、直接的に、ＭＰＥＧ－２デコーダ９にコンテンツデータ（Ｄａｔａ）を送出してディスプレイ１０ａへの再生出力を行わせる場合には、受信側のＭＰＥＧ－２デコーダ９が、図におけるＨＤＤ６と等価な動作を行うことで、ＩＲＤ１とＭＰＥＧ－２デコーダ９は互いに他を認証できるとともに、ＰＣＩバス５を流れるコンテンツデータは両者の固有の共通キーＫにて暗号化された状態となるため、ＰＣＩバス５を流れるコンテンツデータの不正使用を確実に防止できる。

【００５８】以上のように、本実施の形態の交信では、通信路（ＩＥＥＥ１３９４バス２やＰＣＩバス５）には双方の公開鍵と暗号化データしかやり取りされない。また、共通鍵は暗号化されてやり取りされる他、公開鍵から秘密鍵を求めることは出来ない。これらより、データを盗んでも鍵が分からないため復号は出来ない。従って、データの不正コピー等の不正使用を確実に防止できる。

【００５９】図２の例では、アルゴリズムの最後で、実

際のデータの暗号化には共通キーＫを用いる暗号アルゴリズムを用いている。これは、通常、公開暗号鍵アルゴリズムは極めて速度が遅く、映像データ等のコンテンツなどの多量のデータをやり取りするには適していないためである。すなわち、本実施の形態では、認証は公開暗号鍵で行い、データの暗号化は共通キーＫで行い、共通キーＫのやり取りは認証に基づいた公開暗号鍵でやり取りする、という手法を取っている。将来、公開暗号鍵アルゴリズムが高速になった際には、全部を公開暗号鍵で行うことも本発明に含まれる。

【００６０】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００６１】たとえば、上述の例では、不正使用からの保護対象として、コンテンツ等のデータに適用した場合について説明したが、これに限らず、たとえば、ＩＲＤ１経由で配付されるゲームやビジネス等のソフトウェア等の保護にも適用することができる。その場合には、当該ソフトウェアの受信部分（たとえばＩＲＤ）から実行部分（ＣＰＵや主記憶、あるいはソフトウェア実行専用に接続された周辺機器）までの間におけるデータ転送経路における暗号化を行うようにすればよい。

【００６２】

【発明の効果】本発明の情報処理装置によれば、パーソナルコンピュータ等の情報処理機器にて取り扱われるコンテンツデータやプログラム等の不正使用を防止することができる、という効果が得られる。

【００６３】本発明の情報処理装置によれば、不正使用を懸念することなく、パーソナルコンピュータ等の情報処理機器を用いたコンテンツデータやプログラム等の処理システムの構築を実現することができる、という効果が得られる。

【図面の簡単な説明】

【図１】本発明の一実施の形態である情報処理装置の構成の一例を示す概念図である。

【図２】本発明の情報処理装置にて使用される認証アルゴリズムの一例を示すフローチャートである。

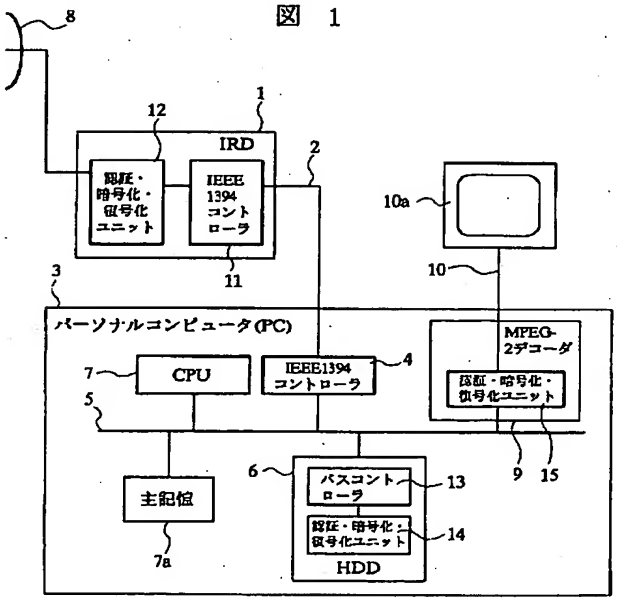
【図３】本発明の情報処理装置におけるデータの暗号化の過程の一例を示す概念図である。

【符号の説明】

１…ＩＲＤ（周辺機器）、２…ＩＥＥＥ１３９４バス、３…パーソナルコンピュータ、４…ＩＥＥＥ１３９４コントローラ、５…ＰＣＩバス（情報伝送路）、６…記憶装置、７…ＣＰＵ、７ａ…主記憶、８…アンテナ、９…ＭＰＥＧ－２デコーダ（周辺機器）、１０…アナログＴＶ出力、１０ａ…ディスプレイ、１１…ＩＥＥＥ１３９４コントローラ、１２…認証・暗号化・復号化ユニット（第１の機能、第２の機能）、１３…バスコントローラ、１４…認証・暗号化・復号化ユニット（第１の機能、第２の機能）、１５…認証・暗号化・復号化ユニット（第１の機能、第２の機能）。

【図１】

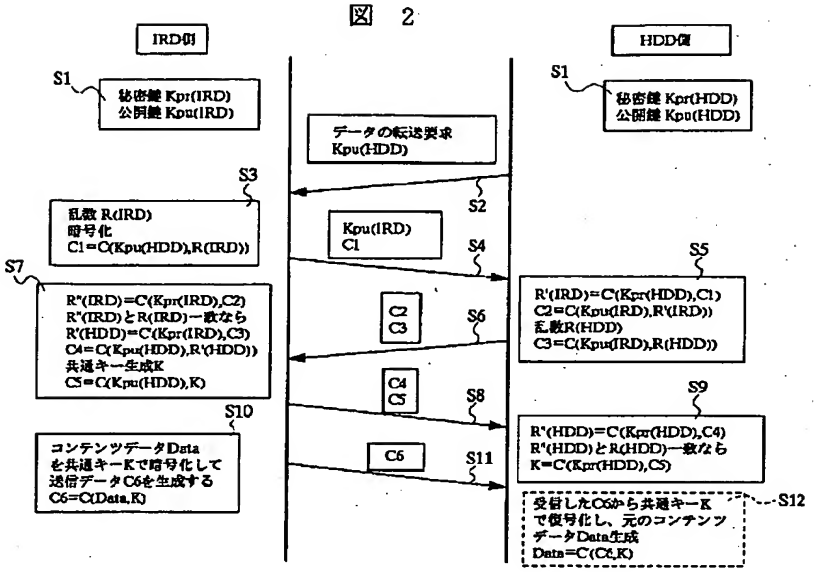
図　1



2：IEEE1394バス　　10：アナログTV出力
5：PCIバス　　10a：ディスプレイ
8：アンテナ

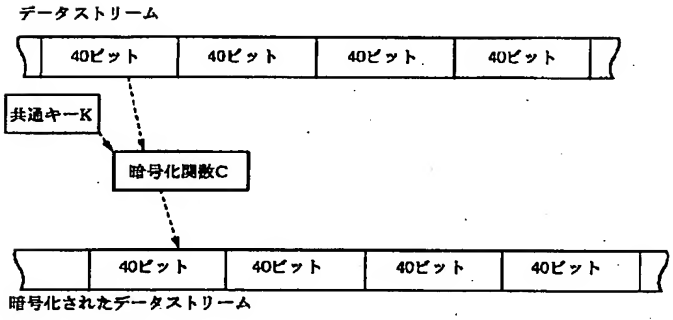
【図２】

図 2


IRD側
HDD側
S1
秘密鍵 Kpr(IRD)
公開鍵 Kpu(IRD)
S1
秘密鍵 Kpr(HDD)
公開鍵 Kpu(HDD)
データの転送要求
Kpu(HDD)
S2
S3
乱数 R(IRD)
暗号化
C1=C(Kpu(HDD),R(IRD))
Kpu(IRD)
C1
S4
S5
R'(IRD)=C'(Kpr(HDD),C1)
C2=C(Kpu(IRD),R'(IRD))
乱数R(HDD)
C3=C(Kpu(IRD),R(HDD))
S7
R''(IRD)=C'(Kpr(IRD),C2)
R''(IRD)とR(IRD)一致なら
R'(HDD)=C'(Kpr(IRD),C3)
C4=C(Kpu(HDD),R'(HDD))
共通キー生成K
C5=C(Kpu(HDD),K)
C2
C3
S6
C4
C5
S8
S9
R''(HDD)=C'(Kpr(HDD),C4)
R''(HDD)とR(HDD)一致なら
K=C'(Kpr(HDD),C5)
S10
コンテンツデータData
を共通キーKで暗号化して
送信データC6を生成する
C6=C(Data,K)
C6
S11
S12
受信したC6から共通キーK
で復号化し、元のコンテンツ
データData生成
Data=C'(C6,K)

【図３】

図 3


データストリーム
40ビット
40ビット
40ビット
40ビット
共通キーK
暗号化関数C
40ビット
40ビット
40ビット
40ビット
暗号化されたデータストリーム